Human-centric Personal Data Protection and Consenting Assistant Systems: Towards a Sustainable Digital Economy

Soheil Human * Rainer Alt + Hooman Habibnia * Gustaf Neumannn*
*Institute for Information Systems and New Media
Vienna University of Economics and Business, Austria
soheil.human@wu.ac.at, gustaf.neumann@wu.ac.at
+Information Systems Institute
Leipzig University, Germany
rainer.alt@uni-leipzig.de

Abstract

With the growing digital transformation, increasingly more personal data is produced, collected, shared, and used. Online privacy has become one of the most significant challenges for co-creating digital artefacts in a sustainable digital world. This paper presents the results of a representative study on online privacy conducted in Austria, which shows a growing need for personalized and human-centric sociotechnical solutions which empower humans to exercise their rights to online privacy, consenting and agency. We call such systems Personal Data Protection and Consenting Assistant Systems (PDPCAS). Using a human-centric perspective on privacy and consenting, which is inspired by recent advancements in cognitive sciences and sociology of science and technology, as well as the results of our representative study, combined with the results of a set of interdisciplinary expert interviews, we provide a reflection on PDPCASs, which mainly includes the functional and non-functional requirements of such systems. Based on the results of our studies, we reflect on the main challenges for the development and adaptation of PDPCASs. We argue that besides the absence of supporting automation standards, the lack of enforceability, and the technical complexities of developing human-centric PDPCASs, the user-acceptance and user experience design pose significant challenges to realizing these systems in practice. Finally, the paper provides a short reflection on the importance of human-centric PDPCASs for the co-creation of a sustainable digital economy.

1. Introduction

Our society is becoming increasingly digital and online. In particular, the developments surrounding the COVID-19 global pandemic–which compelled many people, governments, companies, schools, universities, etc. to embrace an almost entirely online life–made it even more clear how online technologies are co-producing our personal and social lives as well as our professional interactions while blurring the lines between the two. As the prevalence of our online activities becomes more and more prominent, so do the concerns about *digital privacy* and *online consent* (see e.g. [1, 2]). Too often, companies follow business models that consider humans' personal data as a resource that can be owned and controlled by them rather than the data subjects [1, 3]. Collecting and processing such vast amounts of personal data, if done incorrectly, can cause many negative social and technical consequences (see [2, 4] for a short overview), including the invasion of people's privacy and agency. As a result, regulations such as the European General Data Protection Regulation (GDPR) [5] have tried to implement a better practice of the right to digital privacy. Nevertheless, despite new legislations, it seems that users do not have actually the ability—and have not been fully empowered [6] by interdisciplinary solutions—to thoroughly exercise their digital rights as granted by laws [4]. The challenges of practising users' rights to privacy and consenting are highly problematic for both users and data controllers: users face numerous difficulties in accessing their rights and data controllers struggle to provide them effectively as doing so is slow, complex, and time-consuming. More often than not, the existing solutions do not take into account human-centric aspects of privacy and consenting, i.e. the cognitive, collective, and contextual dimensions [4], although these dimensions have been frequently studied and reported in academic literature (see, e.g. [2, 4, 7, 8, 9, 10, 11]).

The contribution of this paper is four-fold: I) while the challenges of online privacy denote a well-researched field, we will present and use the results obtained from a representative survey on online privacy conducted in Austria to argue that despite all previous multidisciplinary efforts, users have *still* difficulty managing their online privacy and *consenting*–more than three decades into the age of the Web–and therefore *novel* Personal Data Protection

URI: https://hdl.handle.net/10125/79913
978-0-9981331-5-7

and Consenting Assistant Systems (PDPCASs) should be developed—together with other sociotechnical and socio-legal means—to empower end-users in managing their online privacy and consenting. II) we will combine the results of our representative survey with the results of a set of expert interviews, as well as a human-centric framework on privacy and consenting (proposed by [4]) to provide a list of the most important end-user-centric functional and non-functional requirements [12, p.36] that PDPCASs are supposed to accomplish or fulfil. III) We will discuss the challenges of the realization of such systems based on the literature and the data from the representative survey. IV) while the main sections of this paper can contribute towards the realization of PDPCASs, we will also provide a short discussion on the contribution of this paper to the more general literature dealing with sustainability and human-centricity of information systems and the digital economy.

2. The Need for Data Protection and Consenting Assistant Systems

Privacy is a human right (see, e.g. the GDPR, Recital 1 [5]). The invasion of humans' online privacy influences individuals and has many negative societal and economic consequences (see [2] for a short discussion). Various difficulties that individuals face in their efforts for *a personal management of their online privacy* have been well studied and reported in the literature (see [2, 4] for an overview). As a result, many scientists have called for novel interdisciplinary solutions to support and empower [6] end-users to access their fundamental right of online privacy. Among others, this includes societal measures (such as better public education and increase of public awareness [13, 14, 15, 16]), economic measures (such as novel business models [17]), political and legal measures (such as new regulations and standards [18, 19]), and technological solutions (such as privacy enhancement technologies [20], privacy by design approaches [21], user-centric personal data ecosystems [22], personal vaults [23], personal databoxes [24], encryption-based architectures for management of personal data [25], browser-plugins for blocking advertisements and tracking cookies, automated mechanisms for the communication of users' privacy decisions [26], etc).

While some of these proposed approaches and technologies are more than 20 years old (e.g. [20]), it seems that even in 2021, end-users still need to be empowered by multidisciplinary means to be able to manage their online privacy. To provide *objective evidence* to prove this claim and to show that even the two decades of advancement in various types of technologies, regulations, and standards have not fully solved the problem of online privacy, we conducted an online representative survey (n=338) on online privacy in Austria in 2020 and 2021 to study the end-users' knowledge, attitude, expectations, and reported behaviour. The survey provides a representative sample of different social groups based on the participants' age, gender, federal state (German: *Bundesland*) of residence, and their level of education. Participants could do the survey either in German or in English. Figure 1 shows the distribution of the participants based on their age and gender. Figure 2 groups the participants according to their federal state of residence.

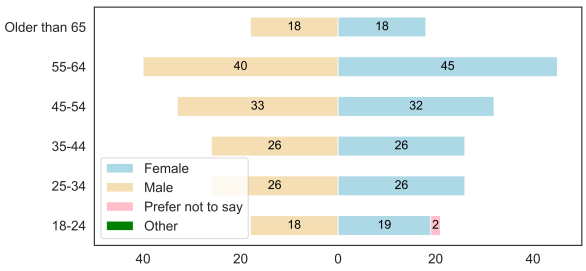

Figure 1. The distribution of the participants based on their gender and age

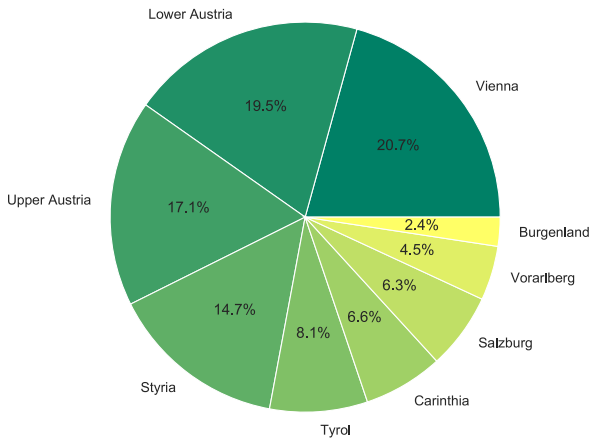

Figure 2. Participants represented according to their federal state of residence

Figure 3 summarizes the answers to the questions that are most relevant to the topic of this paper. As shown, only a small portion of participants said they were "very confident" about different aspects that can be seen as *self-reported* knowledge of (or expertise in) managing their online personal data

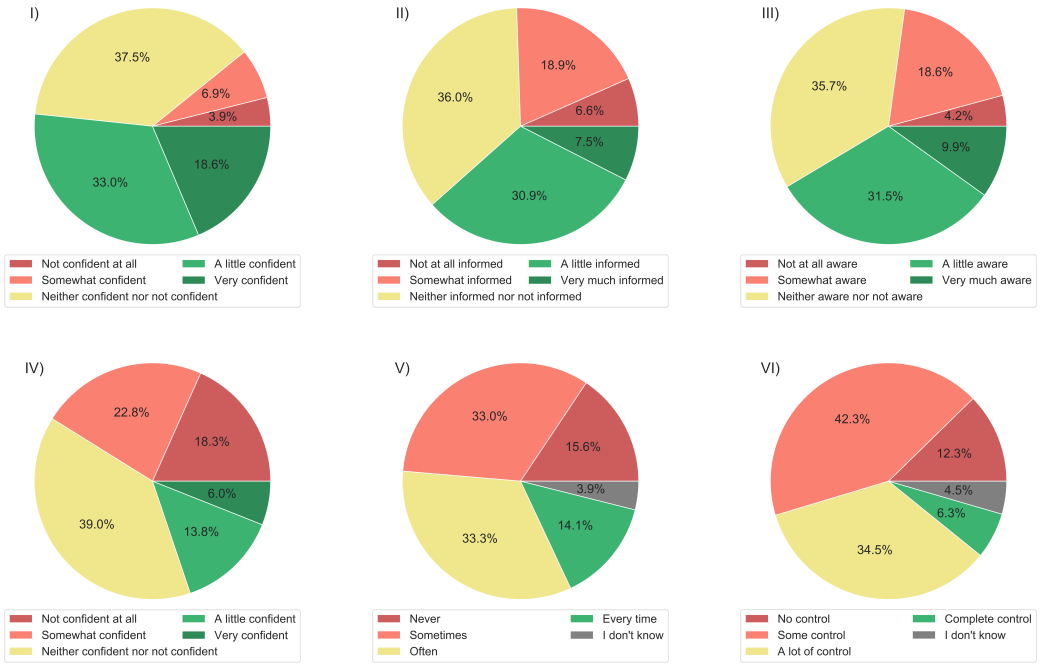

Figure 3. I: "How confident are you with using digital technologies?", II: "Would you say that you are informed of your legal rights to digital privacy?", III: "Would you say that you are aware of what information is collected by the services you use?", IV: "How confident are you about your knowledge of profiling?", V: "Do you read the privacy policies before using a digital service?", VI: "How much control do you 'feel' you have over the information you provide online?".

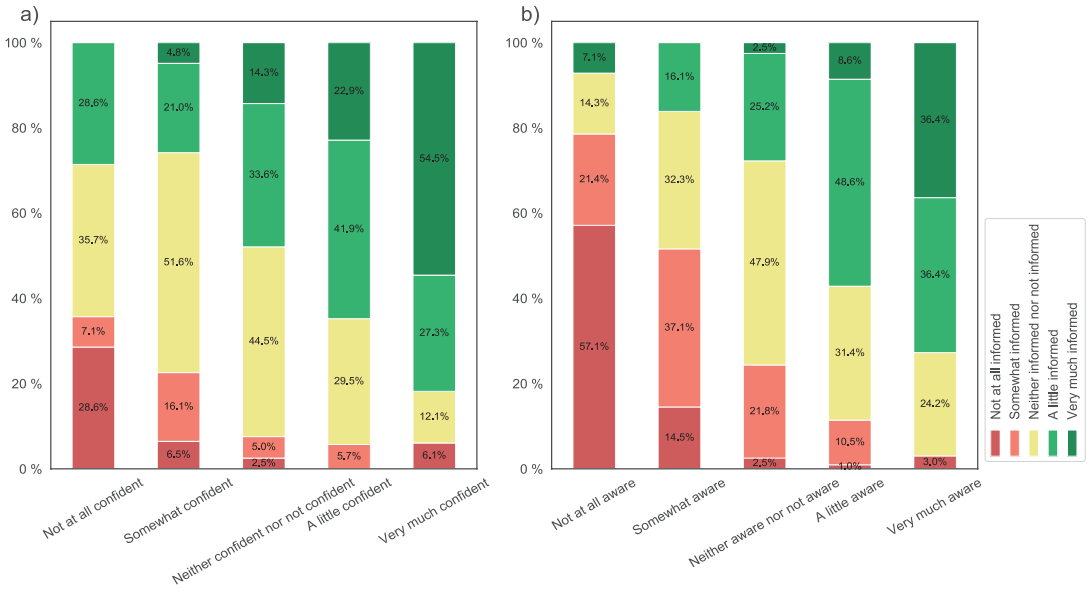

Figure 4. The overlap between the questions I & II, and III & II

or online privacy. In most cases, over 50% of the participants regarded themselves as "not confident[1] at all", "somewhat confident", or "neither confident nor not confident". This clearly shows the need for users to be empowered by sociotechnical means in terms of managing of their online privacy.

This urge becomes more evident if we focus on the group who reported themselves as "the least confident" with using digital technologies (also known as technologically *underprivileged* people; question I), or least informed about their legal rights to digital privacy (question II). The correlation analysis between the answers to questions I and II, as well as between the answers to questions III and II (presented in Figure 4) makes it explicit that those who regard themselves as not well informed of their legal rights to digital privacy have higher chances to also feel less confident about using digital technologies and less informed of what information is collected by the services they use. These people can be categorised as the most vulnerable group of users in need of additional support. Interestingly, Figure 4 also shows that considering oneself well-informed about their rights to digital privacy does not necessarily imply the persons' technical expertise in managing their personal online privacy. Overall, the results of the representative study show that people should be empowered regarding the management of their online privacy.

Besides the representative survey, we also conducted a small (informal) exploratory study in which participants who attended privacy-related events ($n \approx 187$) were verbally asked: "Can you list (using your own memory, digital tools, or other means) at least 50% of the online consents that you have given during the last month?" As expected, no one ever claimed that they could do that. The case of *consenting*[2] is an important aspect of privacy management: According to the GDPR (Article 6 [5]) there are different *legal bases* for a *lawful* practice of personal data processing. End-users' consent is *only one of these possible bases*. However, consents are still widely obtained (e.g. in the form of cookies banners or privacy policies). However, users usually do not have enough cognitive capacities, time, expertise, or motivation to be involved in online *consenting* adequately. Moreover, *consenting* is widely currently practiced as an *individual task*, which ignores the *collective* aspects of online *consenting* and puts a lot of load on the shoulders of each end-user [27]. Furthermore, many of the existing consent-obtaining mechanisms (e.g. cookie-banners) include nudging mechanisms (sometimes called *dark patterns*) that can even make *consenting* more unfair and difficult for the end-users [4]. The existing technical solutions are either data-controllers-centric (e.g. the *Consent Management Platform* (CMPs)) or are mainly developed for blocking tracking (e.g. browser-plugins like *Privacy Badger*[3]) and do not empower the end-users regarding an advanced management of their consents (and potential objections). Considering this, we argue that users need to be at least empowered by tools that can enable them to keep track (and manage) their online consents. Such tools can be considered one of the simplest forms of PDPCAS. However, a better solution, clearly, will be developing *more advanced* human-centric PDPCAS, which can ultimately empower end-users regarding the management of their online privacy and consenting.

In summary, our studies show that almost everyone needs at least Personal Data Protection and Consenting Assistant Systems that can keep track of their online consents. There is, at least, one portion of society (e.g., *technologically underprivileged people*) that need to be empowered regarding their online privacy using tools that are more than *consent-tracking systems*. Therefore, we propose that (together with other complimentary socio-technical measures), Human-centric Personal Data Protection and Consenting Assistant Systems can be considered required measures to enable people to practice and protect their right to privacy.

3. A Human-centric Perspective on PDPCASs

Like most other sociotechnical information systems, one of the essential steps towards developing PDPCASs is assessing their functional and non-functional requirements [12], i.e., *what should they be* and *what should they do*. In the following, we try to contribute to this critical need. For this purpose, we first reflect on PDPCASs based on the framework proposed by Human and Cech [4], then describe our methodology of a qualitative study (expert interviews) on functional and non-functional requirement assessment of PDPCASs. Finally, we present the result of our assessment.

After a discussion on the *nature* of online privacy and *consenting* based on the interdisciplinary literature on online privacy, cognitive science, and the sociology of science & technology, Human and Cech [4], propose a basic human-centric framework for empowering

[1] the adjective "confident" should be replaced with similar adjectives such as "aware", or "informed" based on the target question.

[2] we should consider that while *consenting* is an important aspect of online *privacy*, *consents* can also be obtained from users regarding non-privacy-related matters.

[3] https://privacybadger.org

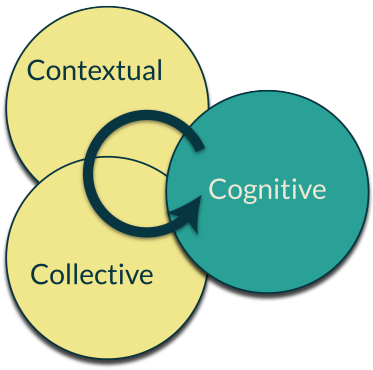

Figure 5. A simple visualization of the socio-cognitive dimensions of online privacy; the social dimensions are shown in light colour [4]

end-users in the context of the management of their online privacy wherein online privacy-related *actions* (e.g. the action of online *consenting*) are considered *socio-cognitive actions* which include *cognitive*, *collective*, and *contextual* dimensions (see Figure 5).

According to [4], "if we accept that 'the individual end-users and their needs and values, as well as the environment (including socio-economical contexts, other actors, etc) and technologies they interact with, continuously co-create the [...] end-user empowerment' [28] (see also [2, 29]), only an approach which considers all these different involved dimensions can truly enable human empowerment." Such an approach is called *human-centric*, wherein individual (cognitive) and social (collective & contextual) dimensions of every end-user and all end-users combined are taken into account when an information system–a PDPCAS in our case–is designed, implemented, evaluated, and released [4].

Based on this perspective, which is inspired by the *enactivism* approach in cognitive science [30, 31, 32], considering humans "*cognitive systems enacting in their socio-contextual environments* provides a framework for empowering them based on their socio-cognitive needs, values, capabilities and limits" [4]. If applied to the development (or co-creation) of PDPCASs, this perspective will encourage designers and developers to consider the socio-cognitive aspects of end-users (and their interactions with information systems) in the development of new PDPCASs. Designers or developers of human-centric PDPCASs should continuously evaluate if different cognitive, collective, and contextual dimensions of the actions that are expected to adequately be conducted *via or by PDPCASs* have been considered in the PDPCAS that they have designed or developed. We propose that without considering a human-centric perspective, which focuses on the multidimensionality of human actions (or *enactions*), research on (or development of) complex empowering technologies such as advanced forms of PDPCASs, that should be able to serve *diverse users* in different contexts, is hardly an achievable task. This is one of our motivations for aligning the identified requirements with the three dimensions of human-centric privacy and consenting framework, as discussed below and represented in Table 1.

3.1. Expert Interviews

Considering the described human-centric framework, as well as the need for the assessment of functional and non-functional requirement of PDPCASs, we conducted a set of interdisciplinary expert interviews. An interdisciplinary group (n=15) of experts from digital law, computer science, information systems, philosophy of technology, and STS participated in the interviews. Following a well-defined semi-structured interview guideline, in order to reduce the potential *priming effect*, PDPCASs were not directly mentioned in the questions. For example, it was asked, *"which tools and means have the potential to contribute towards empowering individuals to exercise control over (and benefit from) their personal data? Please describe them. (We encourage you to think about tools and means that can be realized within the next 2 to 5 years)".* After the data collection, following a data analysis plan and using *Grounded Theory* (see [33]), independent coders (annotators) analysed the data. The data analysis was done in two phases: (1) initial coding and (2) focused coding. After the second coding, theoretical coding was applied in order to subsume the emerged concepts into categories and find hypothesis in the data (including the alignment of the identified requirements with the three dimensions of human-centric privacy and consenting framework described above, i.e., cognitive, collective, and contextual dimensions). Then the results were sent to the interview partners for evaluation. They were also later provided with input about the human-centric framework, PDPCASs, and the results of the data analysis and asked to provide their own view about the alignment of different requirements with the three target dimensions.

3.2. Human-centric Functional and Non-Functional Requirements

Given the discussed aspects and the results of our studies, we summarize the list of assessed functional and non-functional requirements of PDPCASs in

Table 1. The most important functional and non-functional requirements of PDPCAS, aligned with the three dimensions of the human-centric privacy and consenting framework (the colour density represents the significance of each dimension in the realization of the requirements)

Non-functional Requirements				
Name	**Description**	**Cog.**	**Coll.**	**Cont.**
Pluralist	PDPCASs should consider the diversity of users, laws, perspectives, used technologies, surrounding technologies, use-cases, etc.			
Enactivist	PDPCASs should consider enactive interactions of users with their [digital] environments and take it into account that humans and technologies *co-produce* each other.			
Personalized	PDPCASs should consider each user's dispositional and situational needs, values, preferences, knowledge, expertise, limits, etc.			
Understandable	Different aspects of PDPCASs should not only be transparent and explainable, but also understandable for their end-users (or individuals or organizations trusted by the end-users).			
Controllable	PDPCASs should give back the control of online privacy and consenting to the user and be under their control.			
Lawful	PDPCASs should consider different regulations and legal frameworks and be themselves lawful (and enforceable, when needed).			
Beneficial	PDPCASs should give a higher priority to their *end-user*'s benefit (over the other stakeholders' benefit) while respecting collective and societal values and regulations.			
Accountable	The accountability of PDPCASs and different human and non-human actors involved in their development and application should be clear.			
Ethical	The co-creation of PDPCASs—and their application—should be ethical. PDPCASs, their components and surrounding technologies should be based on (and sensitive to) diverse values.			
Auditable	Different aspects and components of PDPCASs should be auditable by independent interdisciplinary experts.			
Integrable	PDPCASs should be integrable with various devices, tools, services, sensors, software, and apps. They should be able to work in the users' *data environments*.			
Functional Requirements				
Name	**Description**	**Cog.**	**Coll.**	**Cont.**
Consenting	PDPCASs should provide human-centric means for consenting, and expressing end-users' personal data and privacy-related decisions and preferences.			
Representing	PDPCASs should be able to represent end-users' privacy and consenting decisions—and all related information and knowledge—as data, visualizations, UI elements, semantic structures, etc.			
Communicating	PDPCASs should be able to communicate end-users' privacy and consenting decisions (or related information, knowledge, or data) with other actors.			
Memorizing	PDPCASs should be able to memorize end-users' privacy and consenting decisions (and related information, knowledge, or data).			
Retrieving	PDPCASs should be able to retrieve end-users' privacy and consenting decisions (and related information, knowledge, or data).			
Automatizing	PDPCASs should [semi-]automatize different process and tasks involved in the management of end-users' privacy and consenting.			
Cog. support	PDPCASs should provide [semi]-automated decision supports to reduce users' cognitive tasks of privacy and consenting management.			
Coll. support	PDPCASs should make it possible for the end-users to get support from others (i.e. other trusted end-users, experts, NGOs, etc.).			
Cont. support	PDPCASs should provide end-users with context-sensitive decision support regarding their privacy and consenting management. They should also consider the *contextuality* of consenting.			
Explaining	PDPCASs should provide means for explaining involved aspects, e.g. the PDPCAS itself, its components, data, decisions, communications, etc.			

Table 1 and envision a human-centric perspective on PDPCASs as discussed below:

A Human-centric Personal Data Protection and Consenting Assistant System (Human-centric PDPCASs) supports the end-user[4] to "memorize" or "remember" the consents or other privacy-related information and decisions about their "online life", e.g. it keeps a record of privacy-related decisions and interactions of the users and the responses of the data-controllers, or it keeps track of personal data that are collected, generated, or shared about the user. It is transparent and understandable for the users and enables them to manage their preferences and decisions and communicate their decisions with other actors in an *automated* manner. It also provides cognitive, contextual, and collective reasoning to support the users in managing or partially automating their online privacy decision-making. Human-centric PDPCASs can become personalized (using explicit settings or learning from the interactions and decisions). They are not only context-sensitive [34], but also can use experts' or peers' inputs to support less-experienced users in a human-centric manner. In summary, the Human-centric PDPCASs function based on the *nature* of human online privacy interactions (summarized above and discussed in [4]) and consider individual, situated and contextual needs and values [2] of their owners, as well as collective inputs from trusted experts or peers.

[4]or their trusted parties, e.g. their family members who support the user, or trusted experts (e.g. NGOs)

4. Challenges for Realization of Human-centric PDPCASs

While the discussed human-centric perspective on PDPCASs and the provided functional and non-functional requirements can be regarded as an important first step towards the realization of such systems, the identification of challenges ahead is also a crucial step in informing the future research directions. We first discuss below the challenges for the realization of Human-centric PDPCASs that identified by our representative research (user-centric challenges). We will then provide an overview of a set of diverse interdisciplinary challenges (inspired by the literature and our qualitative study):

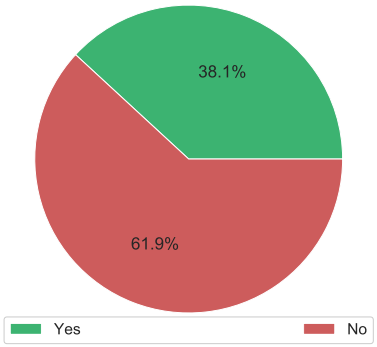

Figure 6. Have you ever considered the privacy aspect when buying an electronic device?

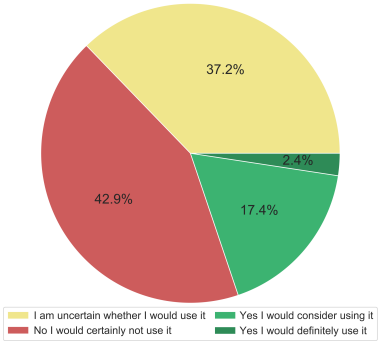

Figure 7. Would you consider using a virtual assistant to manage your privacy preferences, if that technology were offered to you?

4.1. User-centric challenges

End-users' trust and acceptance can be an important success factor of any technology. The current users' knowledge, expertise, needs, habits, attitudes,

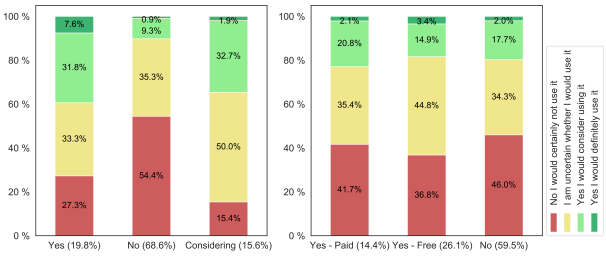

Figure 8. The overlap of "Would you consider using a virtual assistant to manage your privacy preferences, if that technology were offered to you?" with (left) "Do you use any digital assistants on your electronic devices?" and (right) "Do you use any services/technologies to increase your digital privacy?"

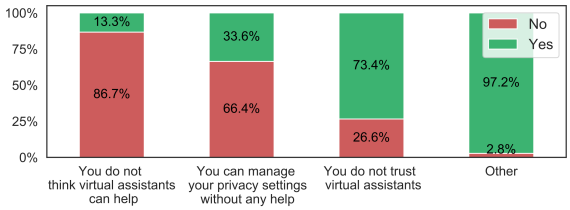

Figure 9. For what reason(s) would you rather not use a virtual assistant for privacy management?

biases, expectations, visions, values or imaginaries can potentially influence if (and to what extent) they accept Human-centric PDPCAS. When participants were asked, "Have you ever considered the privacy aspect when buying an electronic device?" (Figure 6), most of them (61.9 %) admitted that they had not considered the privacy aspect. However, as argued and discussed by Busch, [35] (see also [7, 36, 37, 38, 39]) this cannot be interpreted as an evidence for claiming that privacy does not matter to people. A more direct question will be more interesting for the case of PDPCASs: "Would you consider using a virtual assistant to manage your privacy preferences, if that technology were offered to you?" As presented in Figure 7, only a small number of participants thought of using PDPCASs. This could potentially be *the biggest challenge* for the realizations of PDPCASs. Interestingly, as it is shown in Figure 8, those users who claimed that they would use a virtual assistant system (e.g. Alexa, Siri), or those who reported that they were already using some services or technologies to increase their digital privacy (e.g. cookie blockers), said that they will not use PDPCASs. These surprising results (see in particular Figure 7) could have been caused by lack of knowledge or awareness of the PDPCASs and their benefits. Figure 9 shows the

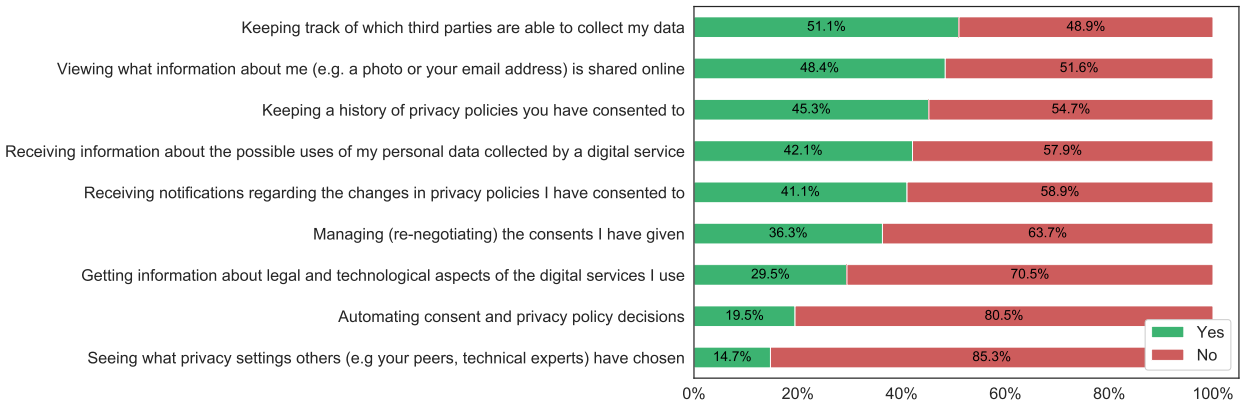

Figure 10. Participants responses to 'Which privacy related tasks would you use your digital assistant for?'

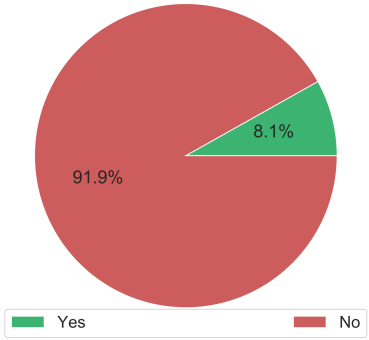

Figure 11. Have you ever sought help with your personal data processing online?

main reported reasons for these surprising findings. It seems that most of the users do not trust *virtual assistance* and regard PDPCASs as a service provided by the existing virtual assistants. Therefore, they prefer not to use such services. A clear framing of Human-centric PDPCASs and making an explicit distinction between them and the main-stream virtual assistants can contribute to tackling this challenge: i.e. the construction and communication of an appropriate *imaginary* (i.e. shared vision) regarding Human-centric PDPCASs can be a crucial users' acceptance factor.

Understanding users' expectations can also be a significant input for the design and development of Human-centric PDPCASs. Figure 10 shows for which privacy related tasks users would use their digital assistant system, assuming that they have decided to use the system. Interestingly, in line with our exploratory study, the results show that the two most demanded tasks are *keeping the track of consents* as well as that of *shared personal data*. As proposed in the previous section, one of the simplest types of PDPCAS can provide a consent-tracking system.

The collective dimension of privacy, which also includes getting support from peers and experts, is not well received by users. This is shown in both Figures 10 and 11: On the one hand, the majority of participants responded that they had *never* sought help with their personal data processing online. On the other hand, they said that they do not intend to use digital assistance to receive collective support. This may be due to the current dominant *individualistic* approach towards online privacy that has shaped the participants' attitude and perspective. Research, however, (see [9, 10, 40, 8]), has shown the positive impact of collective approaches towards privacy management. Again, we propose that this *non-knowledge* can be tackled by appropriate framing and communication of human-centric PDPCAS.

4.2. Other diverse interdisciplinary challenges

Development of PDPCASs as *pluralist* systems is a challenging prerequisite of a *human-centric* perspective (as it is discussed in [2, 4, 41]). This pluralism includes different *human* and *non-human actors* [42, 43], ranging, e.g., from diversity in users and their situated needs, values, expertise, and limits, to diversity in computational components that are used in the development of the PDPCASs (see [2] for a discussion on the latter point).

Technical complexity of Human-centric PDPCAS is highly dependent on the functionalities of the system. The development of a simple Human-centric PDPCAS that can only support users to keep track of their consents is still a complex task. However, the realization of a system that embodies more advanced functionalities, such as predictive models to semi-automatise the process of

consenting, or to manage (e.g. withdraw or modify) the given consents or access-permissions is even more complex. Human-centric PDPCASs can even include computational cognitive models of their users' situated needs and values to empower them effectively and in a situated and case-based manner. The development of such cognitive models (e.g. [30]), however, is a very challenging task and needs further interdisciplinary research.

The lack of required standards, protocols, and regulations could be another barrier to realizing Human-centric PDPCASs. PDPCASs should be able to communicate with various services and even express users' decisions in a *legally enforceable manner*. The failure of previous attempts at establishing automated means for the communication of privacy-related meta-data, or users' privacy decisions[5] indicates that complementary regulations, enforceable standards, and novel sociotechnical mechanisms (e.g. [26]) are needed to support PDPCASs in *human-centric personal data and privacy environments*.

Further challenges identified by the study were, among others: *user experience (UX)*, *accountability*, *transparency*, *understandability*, *controllability*, *fairness*, *inclusiveness*, *security*, *stakeholders' conflicts of interest*, *problematic business models*, and *industry readiness*.

5. Conclusion

The results of our exploratory and representative studies in Austria show that people need to be empowered to protect their personal data. In this paper, we used a human-centric framework and the input obtained from our quantitative and qualitative studies to propose that human-centric PDPCASs can be considered one of the solutions for enabling users to manage their online privacy. Moreover, we provided a set of the most important functional and non-functional requirements of PDPCASs. We also reflected on their development and adoption challenges, which can contribute to realizing such systems.

Considering that: (1) personal data and personalized services are two essential drivers of the digital economy, (2) human values—including privacy and agency—must be carefully respected in any sustainable digital transformation initiative, and (3) human-centric interdisciplinary means are needed to empower users to express and *enact* their values, we believe that the development of PDPCASs–besides other complementary solutions–can contribute towards a more sustainable [44] digital world.

[5] e.g. the missing acceptance of the W3C DNT (Do Not Track) signal

6. Acknowledgement

We acknowledge the comments, suggestions, and contributions of our colleagues, in particular Rita Gsenger, Mandan Kazzazi, and Ozan Aybar.

This publication is partially funded by the Vienna University of Economics and Business (WU Wien), project *Human—Digital:Sustainability*.

References

[1] S. Zuboff, "Big other: surveillance capitalism and the prospects of an information civilization," *Journal of Information Technology*, vol. 30, pp. 75–89, Mar. 2015.

[2] S. Human, G. Neumann, and M. F. Peschl, "[how] can pluralist approaches to computational cognitive modeling of human needs and values save our democracies?," *Intellectica*, no. 70, pp. 165–180, 2019.

[3] S. Zuboff, *The age of surveillance capitalism: The fight for a human future at the new frontier of power*. Profile Books, 2019.

[4] S. Human and F. Cech, "A human-centric perspective on digital consenting: The case of gafam," in *Human Centred Intelligent Systems*, pp. 139–159, Springer, 2020.

[5] EU, "Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing," *Official Journal of the European Union*, pp. 1–88, 2016.

[6] R. Gsenger, S. Human, and G. Neumann, "End-user empowerment: An interdisciplinary perspective," in *53rd Hawaii International Conference on System Sciences, HICSS 2020, Maui, Hawaii, USA, January 7-10, 2020*, pp. 1–10, ScholarSpace, 2020.

[7] A. E. Marwick and D. Boyd, "Privacy at the margins—understanding privacy at the margins—introduction," *International Journal of Communication*, vol. 12, p. 9, 2018.

[8] T. Lehtiniemi and Y. Kortesniemi, "Can the obstacles to privacy self-management be overcome? Exploring the consent intermediary approach," *Big Data & Society*, vol. 4, no. 2, p. 1—11, 2017.

[9] S. Das, A. D. Kramer, L. A. Dabbish, and J. I. Hong, "The role of social influence in security feature adoption," in *Proceedings of the 18th ACM conference on computer supported cooperative work & social computing*, pp. 1416–1426, ACM, 2015.

[10] P. Emami Naeini, M. Degeling, L. Bauer, R. Chow, L. F. Cranor, M. R. Haghighat, and H. Patterson, "The influence of friends and experts on privacy decision making in iot scenarios," *Proceedings of the ACM on Human-Computer Interaction*, vol. 2, no. CSCW, p. 48, 2018.

[11] N. Kirchner, S. Human, and G. Neumann, "Context-sensitivity of informed consent: The emergence of genetic data markets." Workshop on Engineering Accountable Information Systems. European Conference on Information Systems - ECIS 2019, June 2019.

[12] R. Fulton and R. Vandermolen, *Airborne Electronic Hardware Design Assurance: A Practitioner's Guide to RTCA/DO-254*. CRC Press, 2017.

[13] K. B. Sheehan, "Toward a typology of internet users and online privacy concerns," *The Information Society*, vol. 18, no. 1, pp. 21–32, 2002.

[14] V. Steeves, T. Milford, and A. Butts, *Summary of research on youth online privacy*. Office of the Privacy Commissioner of Canada, 2011.

[15] J. C. Andrews, K. L. Walker, and J. Kees, "Children and online privacy protection: Empowerment from cognitive defense strategies," *Journal of Public Policy & Marketing*, vol. 39, no. 2, pp. 205–219, 2020.

[16] I. Sander, "Critical big data literacy tools—engaging citizens and promoting empowered internet usage," *Data & Policy*, vol. 2, 2020.

[17] D. Uribe and G. Waters, "Privacy laws, genomic data and non-fungible tokens," *The Journal of The British Blockchain Association*, p. 13164, 2020.

[18] S. Pereira, J. O. Robinson, H. A. Peoples, A. M. Gutierrez, M. A. Majumder, A. L. McGuire, and M. A. Rothstein, "Do privacy and security regulations need a status update? perspectives from an intergenerational survey," *PloS one*, vol. 12, no. 9, p. e0184525, 2017.

[19] R. Butarbutar, "Initiating new regulations on personal data protection: Challenges for personal data protection in indonesia," in *3rd International Conference on Law and Governance (ICLAVE 2019)*, pp. 154–163, Atlantis Press, 2020.

[20] I. Goldberg, D. Wagner, and E. Brewer, "Privacy-enhancing technologies for the internet," in *Proceedings IEEE COMPCON 97. Digest of Papers*, pp. 103–109, IEEE, 1997.

[21] M. Langheinrich, "Privacy by design—principles of privacy-aware ubiquitous systems," in *International conference on Ubiquitous Computing*, pp. 273–291, Springer, 2001.

[22] C. Moiso and R. Minerva, "Towards a user-centric personal data ecosystem the role of the bank of individuals' data," in *2012 16th International Conference on Intelligence in Next Generation Networks*, pp. 202–209, IEEE, 2012.

[23] M. Y. Mun, D. H. Kim, K. Shilton, D. Estrin, M. Hansen, and R. Govindan, "Pdvloc: A personal data vault for controlled location data sharing," *ACM Transactions on Sensor Networks (TOSN)*, vol. 10, no. 4, pp. 1–29, 2014.

[24] A. Chaudhry, J. Crowcroft, H. Howard, A. Madhavapeddy, R. Mortier, H. Haddadi, and D. McAuley, "Personal data: thinking inside the box," *Aarhus Series on Human Centered Computing*, vol. 1, p. 4, Oct. 2015.

[25] F. Wang, J. Mickens, N. Zeldovich, and V. Vaikuntanathan, "Sieve: Cryptographically enforced access control for user data in untrusted clouds," in *13th USENIX Symposium on Networked Systems Design and Implementation (NSDI 16)*, pp. 611–626, 2016.

[26] S. Human, M. Schrems, A. Toner, Gerben, and B. Wagner, "Advanced data protection control (adpc)," sustainable computing reports and specifications, WU Vienna University of Economics and Business, Vienna, June 2021.

[27] K. O. Aybar, S. Human, and R. Gesenger, "Digital inequality: Call for sociotechnical privacy management approaches." Workshop on Engineering Accountable Information Systems. European Conference on Information Systems - ECIS 2019, June 2019.

[28] S. Human, R. Gsenger, and G. Neumann, "End-user empowerment: An interdisciplinary perspective," in *Hawaii International Conference on System Sciences 2020*, pp. 4102–4111, 2020.

[29] R. Alt, S. Human, and G. Neumann, "End-user empowerment in the digital age," in *Proceedings of the 53rd Hawaii International Conference on System Sciences*, pp. 4099–4101, 2020.

[30] S. Human, G. Bidabadi, M. F. Peschl, and V. Savenkov, "An enactive theory of need satisfaction," in *Philosophy and Theory of Artificial Intelligence 2017* (V. C. Müller, ed.), (Cham), pp. 40–42, Springer International Publishing, 2018.

[31] A. Clark, *Surfing Uncertainty: Prediction, Action and the Embodied Mind*. Oxford University Press, 2015.

[32] F. J. Varela, E. Thompson, and E. Rosch, *The embodied mind: Cognitive science and human experience*. MIT press, 2017.

[33] K. Charmaz, *Constructing grounded theory: A practical guide through qualitative analysis*. sage, 2006.

[34] S. Human and M. Kazzazi, "Contextuality and intersectionality of e-consent: A human-centric reflection on digital consenting in the emerging genetic data markets," in *1st International Workshop on Consent Management in Online Services, Networks and Things (COnSeNT 2021), co-located with 6th IEEE European Symposium on Security and Privacy (EuroS&P)*, 2021.

[35] A. Busch, "Privacy, technology, and regulation: why one size is unlikely to fit all," *Social dimensions of privacy: interdisciplinary perspectives. Cambridge University Press, Cambridge*, pp. 303–323, 2015.

[36] D. Boyd, *It's complicated: The social lives of networked teens*. Yale University Press, 2014.

[37] D. Boyd and A. Marwick, "Social privacy in networked publics: Teens attitudes, practices, and strategies," in *Decade in Internet Time: Symposium on the Dynamics of the Internet and Society*, (Oxford, UK), 2011.

[38] A. Marwick, C. Fontaine, and D. Boyd, ""nobody sees it, nobody gets mad": Social media, privacy, and personal responsibility among low-ses youth," *Social Media+ Society*, vol. 3, no. 2, p. 2056305117710455, 2017.

[39] A. E. Marwick and D. Boyd, "Networked privacy: How teenagers negotiate context in social media," *New media & society*, vol. 16, no. 7, pp. 1051–1067, 2014.

[40] M. Granovetter, "Economic action and social structure: The problem of embeddedness," *American journal of sociology*, vol. 91, no. 3, pp. 481–510, 1985.

[41] S. Human, G. Bidabadi, and V. Savenkov, "Supporting pluralism by artificial intelligence: Conceptualizing epistemic disagreements as digital artifacts," in *Philosophy and Theory of Artificial Intelligence 2017* (V. C. Müller, ed.), (Cham), Springer, August 2018.

[42] L. John *et al.*, "Actor network theory and material semiotics," *Social theory*, p. 141, 2009.

[43] G. Walsham, "Actor-network theory and is research: current status and future prospects," in *Information systems and qualitative research*, pp. 466–480, Springer, 1997.

[44] S. Human, G. Neumann, and R. Alt, "Human-centricity in a sustainable digital economy," in *Hawaii International Conference on System Sciences (HICSS-54)*, 2021.